

U. S. Government Agency

System Security Authorization Agreement for the Certification and Accreditation of the Agency Computer Center

Version 3.0

April 30, 1998

Prepared under:

Contract Number: XXX

Delivery Order: YYY

Prepared for:

U. S. Government Agency

Prepared By:

Foreword

The System Security Authorization Agreement (SSAA) is a single source for all information pertaining to the certification and accreditation (C&A) process of the U. S. Government Agency (USGA) Agency Computer Center (ACC) automated information system (AIS) resources that are within the scope of this document. As such, it either contains or references all the information necessary for the USGA Responsible Management Official (RMO) to make a decision regarding the accreditation of the USGA ACC.

The SSAA is organized into the six sections described below, and a set of Appendices that, when completed, contain (or reference) all information and documentation needed to support the process. Section 1 contains an identification and description of the AIS resources within the scope of this SSAA. It also addresses the criticality of the AIS resources, the sensitivity of the data processed, stored or transmitted over those resources, and a summary of the concept of operations. Section 2 describes the operating environment of the AIS resources, and includes the threats to that operating environment. Section 3 includes a description of the system architecture associated with all the ACC AIS resources and the boundaries of this C&A effort. Section 4 contains the security requirements for the system to include requirements derived from national, Agency, and local policy as well as special requirements levied by the DAA. Section 5 describes the organization and resources needed to accomplish the C&A of the ACC resources. Section 6 describes the approach, milestones and schedule for the activities associated with each step in the process.

The ACC SSAA, Version 3.0 is the third in a series of three SSAA versions that were produced during the USGA ACC C&A process. The ACC SSAA Version 1.0 documented the initial conditions, understanding of the systems, technical Security Test and Evaluation (ST&E) plan and procedures, and initial ST&E results. The technical ST&E Report at Annex H-A of Appendix H in Version 1.0 contains the results of the original report which was delivered to the Enterprise Services Technology Division (ETSD) at test completion. In order to maintain the integrity of this report, it has not been changed in subsequent versions (2.0 and 3.0). The ACC SSAA Version 2.0 was an interim version that incorporated a refinement of the system description information, interim technical editing, and new Observations which were added at Annex H-B of Appendix H in ACC SSAA Version 2.0. This ACC SSAA Version 3.0 is the final version which supercedes all previous versions. It contains the most current system description data, incorporates the USGA comments on previous versions, additional Issues at Annex H-C of Appendix H, major security deficiencies at Appendix I which are based upon the risk assessment and certification test results at Appendix H, and recommendations for C&A.

ACC SSAA Version 3.0 will be companion document to the AIS Security Plan(s) (OMB A-130 requirement) which pertain to the ACC resources. When changes occur to ACC resources that are significant enough to impact on the security protection described in the AIS Security Plan(s) and the ACC SSAA, then a re-certification and re-accreditation of the USGA ACC may be needed along with appropriate updates to the documents.

The ACC SSAA Version 3.0 contains sensitive information that pertains to ACC system functions, descriptions, and vulnerabilities. To ensure that this document is released to authorized personnel, it is marked "USGA Sensitive" in accordance with the Information Security Goal framework contained in USGA Information Security Manual 2195, 1995 Edition.

Table of Contents

SECTION 1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION	1
1.1 System Name and Identification	1
1.2 Mission	1
1.3 Functional Architecture	2
1.3.1 Functional Description	2
1.3.2 System Capabilities and Interfaces with Other Systems	2
1.3.3 System Criticality	2
1.3.4 Classification and Sensitivity of Data Processed	3
1.3.5 System User Description and Clearance Levels	3
1.4 System Concept of Operations Summary	3
SECTION 2. ENVIRONMENT DESCRIPTION	1
2.1 Operating Environment Overview	1
2.1.1 ATC Building	1
2.1.2 ATC Alarms	1
2.1.3 ACC Guards and Visitor Controls	1
2.1.4 Custodial Personnel	1
2.2 System Development, Integration and Maintenance Environment	1
2.2.1 Configuration Management of Software	2
2.2.2 Configuration Management of Hardware	2
2.3 Threat Description and Environment	2
2.3.1 Threat Description	2
2.3.2 Threat Environment and Points of Failure.	4
2.4 Continuity of Support	4
SECTION 3. SYSTEM ARCHITECTURAL DESCRIPTION	1
3.1 Overview	1
3.1.1 Tier I Architecture	1
3.1.2 Tier II Architecture	2
3.1.3 Tier III Architecture	3
3.2 Certification and Accreditation Boundary	4
SECTION 4. SYSTEM SECURITY REQUIREMENTS	1
4.1 Overview	1
4.2 National Level Security Requirements	1
4.3 Assignment of Responsibilities	1
4.4 USGA Information Security Policy	1
4.5 Security Plan	1
4.6 Review of Security Controls	2
4.8 USGA Security Requirements	2
4.9 System Security Concept of Operations	2
4.10 Network Connection Rules	2
SECTION 5. ORGANIZATIONS AND RESOURCES	1
5.1 Identification of Organizations	1
5.1.1 USGA ETSD Staff	1
5.1.2 The DISA C&A Team	1
5.2 DISA C&A Team Organizational Structure and Management Approach	2
5.3 Organizational Interfaces	2
5.4 Resources and Roles	3
5.5 Certification Team	3

5.6 Other Supporting Organizations or Working Groups	4
5.7 Administrative Issues	4
 SECTION 6. DITSCAP PLAN	 1
6.1 Evaluation Approach	1
6.2 TASK 1: PROGRAM AND PROJECT MANAGEMENT	1
6.2.1 C&A Task Order Management Plan	1
6.2.2 Monthly Status Report	2
6.2.3 Trip Reports	2
6.3 TASK 2: USGA C&A Support	2
6.3.1 SUBTASK 2.1: Definition Phase	2
6.3.2 SUBTASK 2.2: Verification Phase	3
6.3.3 SUBTASK 2.3: Validation	4
6.4 Schedule summary	5

Appendices

Appendix A: Acronym List	1
Appendix B: Glossary of Terms	1
Appendix C: Reference List	1
Appendix D: Requirement Traceability Matrix	1
Appendix E: USGA - ACC Certification and Accreditation Work Plan	1
Appendix F: Risk Assessment	1
Appendix G: Security Test and Evaluation Test Plan and Procedures	2
Appendix H: Security Test and Evaluation Test Evaluation Report	4
Appendix I: System Security Evaluation Report	1
Appendix J: Certification Statement	1
Appendix K: ACC Security Operating Procedures Guide	1
Appendix L: Approval to Operate	1
Appendix M: Rules of Behavior	1
Appendix N: Security Awareness and Training Program	1
Appendix O: Incident Response Program	1
Appendix P: Continuity of Support	1
Appendix Q: Interagency Agreements	2

Figures

Figure 3-1 Major USGA Circuits from Our Town	1
--	---

Tables

Table 3-1 Regional WAN Router Locations	2
Table 3-2 UNIX Production Systems	3
Table 3-3 UNIX Non-Production Systems	3
Table 5-1 USGA ETSD Staff	1

**United States Government Agency
Agency Computer Center
System Security Authorization Agreement**

SECTION 1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

1.1 System Name and Identification

The U. S. Government Agency (USGA) AIS resources that are the subject of this SSAA include those that are installed in, and operated by, the USGA ACC. The ACC is located in the USGA Agency Technology Center (ATC) facility, Our Town (OT), Our State. The AIS resources in the ACC are a complex collection of general purpose systems that provide centralized processing, storing and dissemination of information associated with the Agency's technical research. This includes financial, payroll, travel, personnel, and public access to USGA information.

1.2 Mission and Functions

The mission of the USGA is to permit a coordinated and effective governmental action on behalf of environmental issues. The functions performed by the USGA in the accomplishment of that mission endeavor to abate and control pollution systematically, by proper integration of a variety of research, monitoring, standard setting, and enforcement activities. As a complement to its functions, the Agency coordinates and supports research and anti-pollution activities by state and local governments, private and public groups, individuals, and educational institutions. The USGA also reinforces efforts among other Federal agencies with respect to the impact of their operations on the environment, and it is specifically charged with publishing its determinations when those hold that a proposal is unsatisfactory from the standpoint of public health or welfare or environmental quality.

These functions include gathering, analyzing and storing massive amounts of data and information pertaining to the environment. The effectiveness of the confidentiality, integrity, and availability Information Security Goals provided to the information gathered directly influences the ability of the USGA to perform its functions. The USGA manages and coordinates the resources which provide the automation and telecommunications in the Enterprise Technology Services Division (ETSD) of the Administration and Resources Management structure. Within the organizational framework of the USGA, ETSD provides:

High quality, cost effective computing and telecommunications services to the Agency, Agency contractors, state and local governments, private organizations and citizens in order to provide timely, accurate and understandable information on environmental issues;

Operational oversight for all AIS and voice/data telecommunications resources in the Agency; including Agency-approved and supported computing platforms;

Continually improving information technology capacity and functionality which will enable the best implementation of environmental information delivery systems consistent with Agency needs.

A security directive to insure the operational security of Agency data and computing and telecommunications resources.

The ETSD organization, Figure 1-1, provides these services through the management and operation of the USGA's Agency Computer Center.

1.3 Functional Architecture

The ACC is a collection of general purpose computer systems connected within the ACC and the OT area by local area networks¹, and to Agency sites outside of the ACC and OT area by wide area networks. The computing and telecommunications resources within the ACC are a complex structure of mainframe computer systems; client/ server environments, which provide decentralized processing; data storage peripheral devices; and telecommunications equipment (e.g., switches, routers, hubs, etc.) which link those resources together. All of these resources are designed to provide automated support to users at USGA sites as well as make information available to users from the public sector.

Within the OT area, the ACC provides both centralized/decentralized processing, intranet, and electronic mail (e-mail) capabilities for USGA users. Access by these users to ACC resources is controlled by identification and authentication (I&A) processes that are resident on the mainframes and servers to ensure that only authorized users obtain access to sensitive Agency data. Information is made available to users from the public sector via a series of Internet Web Pages, and Bulletin Boards. Public access does not require I&A. The information at Figure 1-2 is a graphic representation of the structure of the ACC AIS resources. It shows a layered architecture which is intended to facilitate the distribution of information within the USGA and the public sector.

1.3.1 Functional Description

The ETSD management and operation of the ACC supports the USGA and its user community with a variety of capabilities and functions. These include access to Agency information technology, Information Resources Management (IRM) service contracts, and IRM management support services to Agency employees and customers and to external clients and stakeholders. The ACC also provides Help-Desk services for the USGA network resources which provide connectivity to ACC AIS resources, as well as the office automation support for the USGA facilities within the OT area.

1.3.2 System Capabilities and Interfaces with Other Systems

The ACC interface with AIS external to the ACC includes primarily other USGA systems which comprise the wide area network (WAN) environment, and that connectivity which comes from the Internet user community. Details of those interfaces are contained at Section 3.0 of this SSAA.

1.3.3 System Criticality

The AIS resources within the ACC are critical to the operation of the USGA and its user community. This is evidenced by the fact that, with the exception of the Cray computer located in the Their City, Their State facility, the bulk of the USGA processing capability and storage capability is in the ACC.

¹ The C&A boundary is described in Section 3.2 of this SSAA.

While no criticality studies have been conducted, it is generally acknowledged that a catastrophic failure in the ACC would seriously degrade the ability of the USGA to accomplish its mission.

1.3.4 Classification and Sensitivity of Data Processed

All information processed on USGA ACC AIS resources is sensitive. The degree of sensitivity (high, medium, or low) is used to identify specific information security requirements and cost effective measures to protect Agency information. Information sensitivity is determined based on the degree of impact (high, medium, or low) on the Agency's mission that there would be should the availability, integrity, and /or confidentiality protection afforded to the information be compromised. Therefore, the effective confidentiality, integrity, and availability has been declared as Information Security Goals. Information and information systems are sensitive for at least one of three reasons, the need for confidentiality, the need for integrity, and the need for availability. To adequately protect any information assets, both the level of sensitivity (high, medium, or low) and the specific information security goal (confidentiality, integrity, and availability) must be identified.

1.3.5 System User Description and Clearance Levels

Since the ACC does not process classified national security information, USGA users do not have security clearances. Federal USGA employees have been subjected to the new hiring screening process associated with their position. The USGA contractors, however, are required to complete a Standard Form 86 from which a National Agency Check with Inquiry's (NACI) and credit check can be conducted.

1.4 System Concept of Operations Summary

The concept of operations of the ACC includes providing information to the public sector (non-government) to the fullest extent possible, while maintaining a processing environment where USGA personnel (government and authorized contractors) can accomplish the automated processing associated with operations, research and support prescribed by the USGA mission. Information is made available to the public sector without restriction via the Internet (using home pages, Web Servers etc.) and Bulletin Boards.

Information is made available to USGA users by processing applications against databases and by an Intranet which uses Web technology. Authorized USGA users have been given accounts on the various ACC AIS resources. Each authorized user must enter an appropriate I&A before being authorized access to the ACC AIS resources. The requirement for an I&A is the first line of defense for ensuring that only authorized personnel have access to ACC data and AIS resources.

SECTION 2. ENVIRONMENT DESCRIPTION

2.1 Operating Environment Overview

The ACC operating environment is located within the ATC facility of the USGA OT complex. All entrances to the ACC are from within the ATC facility. That is, there are no exit doors from the ACC that lead directly outside of the ATC. The ACC protection mechanisms include physical as well as environmental controls described below.

2.1.1 ATC Building

The ATC is a separate facility located within the OT complex. The ACC is located within the ATC's approximately 500,000 sq. ft. of useable space. There is unrestricted vehicle access to the facility and its adjacent parking lots. The number of exterior perimeter doors available for normal employee use is limited. The entrance door to the ACC is controlled by a badge reader system. Both exterior lighting and camera systems are incorporated into the physical protection of the ATC facility.

2.1.2 ATC Alarms

There are intrusion detection alarms at the perimeter of the ACC.

2.1.3 ACC Guards and Visitor Controls

The ATC facility is manned by armed contract guards 24 hours a day. These guards are responsible for visitor control and access to the building, as well as for conducting random checks of the facility after duty hours. The ATC has a guard dedicated to random patrol of the interior during normal duty hours. Additionally, there is a motorized guard that provides random patrol of the exterior perimeters of both buildings at all times.

All visitors must process through the Visitor Control. A visitors point of contact (POC) must verify the need to visit, and the visitor must have a valid identification which contains a photograph of the individual. If the visitor has no photo identification, then the POC must physically come to the guard station to vouch for the visitor. If a visitor possesses a valid photo identification, then he/she is allowed to proceed unescorted to the POC's office.

2.1.4 Custodial Personnel

Cleaning personnel are allowed unescorted access to all facilities, to include the ACC after a local records check.

2.2 System Development, Integration and Maintenance Environment

The ETSD provides and maintains a processing environment in the ACC that can be used by USGA Program Office personnel to accomplish their mission/functions. That environment includes maintaining the network monitor and control functions that provide connectivity between the ACC and other USGA sites. To the extent necessary, the ETSD staff participates in the planning, acquisition and installation of AIS resources within the ACC, and those of USGA Program Offices that require connectivity to ACC

AIS and network resources. This includes hardware and software resources and the maintenance of databases used to store USGA data.

The USGA Program Offices develop and process the applications software associated with their respective mission/functions in relative autonomy. ETSD staff directly participate in Program Office initiatives only when the application(s) requires special attention from the ACC processing environment to run properly.

2.2.1 Configuration Management of Software

The ETSD staff maintains an informal Configuration Management Program (CMP) over the software (e.g., operating systems, system utilities, databases, etc.) that processes on ACC AIS resources. While there is no formal CMP, there is a formal structure for managing changes to the software that processes on ACC AIS and network resources.

The autonomy of the Program Offices frequently allows for the installation and operation of software on resources outside the ACC in support of specific mission requirements. Any interaction between that Program Office software and the AIS resources in the ACC will require ETSD intervention, since ETSD manages all aspects of the ACC.

2.2.2 Configuration Management of Hardware

The ETSD staff maintains an informal CMP over the hardware, peripherals, and components (e.g., mainframe, servers, communications equipment, etc.) by managing changes to the hardware configuration and architecture within the ACC AIS and network resources.

The autonomy of the Program Offices frequently allows for the installation and operation of AIS resources outside the ACC in support of specific mission requirements. Any interface between those resources and the ACC will require ETSD intervention.

2.3 Threat Description and Environment

This section describes the threats posed to the ACC environment. It is derived from the findings of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) as reported in its Annual Assessment of the Status of National Security Telecommunications and Information Systems Security within the United States Government. This description supplements the threat information presented in USGA Information Security Manual 2195.

2.3.1 Threat Description

The threat of outside intrusion into the ACC system(s) is considered to be high since the USGA mission includes making information available to the public sector and the AIS architecture includes such mechanisms. The integrity of the I&A mechanism is the primary protection for ensuring that the public sector does not access Agency information for which they are not authorized. Therefore, while the external threat is not trivial, the principal threat to USGA data communications and information systems continues to be the insider threat. From a government wide perspective, the NSTISSC assessment is supported by the fact that recent compromises of intelligence and national security information have occurred by of insiders with authorized system access who have disclosed classified information for the

purposes of financial gain, and the potentially volatile behavior of environmental extremist groups reacting to issues confronted by the USGA.

The insider threat arises from multiple sources and is manifested in various ways. Three of these are described below:

- ?? the threat of the cooption of users with authorized access to the system, contractor support personnel, or USGA employees or other USGA contract personnel with physical access to the system components arising from the motivation of financial gain,
- ?? the threat posed by disgruntled employees, especially those who are to be terminated for cause. There is also the threat posed by users of the system who negligently or inadvertently fail to follow security requirements for the handling and labeling of system output or media, or the rules against the introduction of unauthorized software or data imported from unauthorized sources,
- ?? the threat arising from the failure of authorized users to employ proper procedures for the entry or manipulation of system data arising out of negligence or the failure of users to be properly trained in the use and operation of the system.

These insider threats can be manifested in the following ways:

- ?? unauthorized reading, copying or disclosure of sensitive information,
- ?? execution of denial of services attacks,
- ?? introduction into the system of viruses, worms or other malicious software,
- ?? destruction or corruption of data (intentional or unintentional),
- ?? exposure of sensitive data to compromise through the improper labeling or handling of printed output, or
- ?? improper labeling or handling of magnetic media resulting in the compromise of sensitive information.

The co-opted insider would most likely copy to disk and remove from the system any and all types of sensitive information to which such user had authorized access. Such a user might also probe the system in attempt to discover ways to circumvent access permissions and copy and remove from the system sensitive information (e.g., CBI proprietary information, trade secrets, etc.) to which such a user did not have authorized access. One way that this might be attempted by a user who was an extremely sophisticated hacker (or under the direction and control of such a person) might be to discover ways to introduce “sniffer” software into the system to learn the user ID and password of a system administrator or other privileged user, and, by masquerading as such a user, bypass access controls and gain access to the most sensitive information on the system. In most instances of these types of attacks, there could well be attempts to gain unauthorized access to and to modify audit data in order to prevent analysis and detection of the source and nature of the attack. The most serious of all types of possible attacks against the system could be mounted by co-opted systems administration personnel, with their ability to alter or bypass most, if not all, of the system’s technical protection mechanisms.

In addition, either a co-opted insider or a disgruntled employee might attempt denial of service attacks through the manipulation of system software or the malicious introduction into the system of viruses, worms or other destructive software. Authorized users might also maliciously modify data stored on the

system or made available to the public (via Internet, Bulletin Boards, etc.) in order to undermine confidence in the integrity of the system and the accuracy of its stored information. Finally, there could be attempts by insiders with physical access to the ACC, whether authorized users of the system or not, to tap the communications links and record and extract from the system all data passing through those links.

The NSTISSC assessment documents the high level of threat to U.S. Government information and telecommunications systems from hackers, particularly through the medium of the Internet. In the past there have been numerous documented successful hacker attacks on the central switching nodes of the public switched network as well as Web Servers (including Home Pages). The requirement to make information available to the public make the USGA ACC a uniquely vulnerable target for these perpetrators.

While the threat to United States national security telecommunications and information systems from foreign government intelligence activities remains high despite the end of the cold war and the collapse of the former Soviet Union, these intelligence services are not known to target U.S. Government civilian agencies except for the purposes of securing information related to advanced technology or to diplomatic or trade negotiations. Since USGA ACC information systems may process technological information that could fall within this area of interest, the USGA cannot afford to dismiss the possibility of becoming the target of penetration or denial of service attacks by any hostile foreign intelligence services. Despite the possibilities presented above, NSTISSC findings regarding the threat of any successful TEMPEST attack on USGA ACC information systems is adjudged to be extremely low.

The threat of terrorist attack on USGA ACC facilities must be rated as moderate, based upon the recent Oklahoma City bombing and the attack on the World Trade Center and the often unpredictable behavior of environmental extremists. However, proper implementation of the existing physical protection associated with the ACC AIS resources located in the ATC facility should provide adequate protection against inadvertent destruction, and all but the most determined attacker.

The final threat to USGA security that must be considered is the threat posed by fire and natural disasters (e.g. hurricanes, ice storms, flood, earthquake). These threats were included in the Risk Assessments conducted of the ACC facilities as referred to at Appendix F.

2.3.2 Threat Environment and Points of Failure.

The USGA ACC is the focal point for automated processing within the OT as well as other USGA sites within the continental United States. As such, a catastrophic failure of the ACC would result in a serious degradation of USGA processing capabilities. Because of the potential for alternate communications connectivity though some of the T1 circuits not connected to the ACC, minimum capabilities that might withstand such an event would be Lotus Notes and GroupWise, at least through some of the Agency.

2.4 Continuity of Support

The ACC has a formal Disaster Planning and Recovery program. This is a comprehensive program that includes designation of processing priorities, time frames for restoring processing capabilities, alternate processing facilities and bi-annual testing of priority applications. Further, the program is the subject of frequent exercises which include a full activation of the back-up. See Appendix P.

SECTION 3. SYSTEM ARCHITECTURAL DESCRIPTION

3.1 Overview

The USGA ACC is the focal point for the automated support provided to the USGA. It consists of mainframe computers, client/server systems, and large capacity on-line storage as well as cartridge tape storage devices. The resources within the ACC and those within the OT area are connected by local area network architecture. The ACC is linked the AIS resources at other USGA sites by wide area network architecture using high capacity connections that include T1 and T3 circuits shown in Figure 3-1 Major USGA Circuits from Our Town.

<<< Figures removed due to sensitive material. >>>

To provide consistently well-managed information resources, the ETSD acquires, manages, and provides operational oversight for all automated data processing and voice/data telecommunications resources in the Agency. ETSD provides advanced technology, services, and support for USGA to best implement and enhance environmental information deliveries and management.

To perform an analysis of the USGA ACC information technology systems, the systems were placed into various roles and configurations. In accomplishing this, the systems were divided into three tiers. The following sections provide an overview of these tiers. Although some information is outside the scope of this C&A (See Section 3.2), it is provided for better understanding of the overall system.

3.1.1 Tier I Architecture

Tier I computers consist of large scale processors such as the IBM XXX, IBM 4YYX, and a Cray computer system located in Their City, TS. Since the Cray computer is located outside the ACC, it is outside the boundary of the C&A initiative documented by this SSAA. Tier I is shown in Figure 3-2.

The IBM XXX is the primary processor for the ACC. The IBM XXX has 10 processors. Although the computer has been configured with three Logical Partitions (LPAR), all system resources are accessible across all domains. The ACC is currently developing a fourth LPAR, which will be used for the year 2000 issues and contingency testing.

The IBM XXX supports over four hundred applications. These applications are developed; maintained; and submitted by the responsible end-user community. The primary applications include: Application A; Application B; and Application C. In addition to technical applications, the IBM supports financial applications, such as the Contracts Payment System (CPS) which receives EC/EDI contractor invoices through a Tier II UNIX computer and creates an Electronic Funds Transfer directly to the US Treasury.

The IBM 4YYX is an older computer that has been brought into service as a control device for the Storage Silos. This device is also used for contingency testing and planning. The device has no end-users other than the system staff. This system, which was previously connected to the USGA LAN, has since been disconnected from that local area network (LAN).

The operating system which is used for the IBM XXX and the IBM 4YYx is the MVS ESA SP5.2.2. The external security product is the Resource Access Control Facility (RACF). RACF is configured to provide separation of users within the LPARs. Both computers are currently using the Job Entry System 2 (JES2) exclusively.

3.1.2 Tier II Architecture

Tier II computers, shown in Figure 3-3, consist of the WAN, the network management systems, and UNIX systems that provide value added services across the WAN. The WAN topology is a collection of supernodes and regional routers that connect to LAN routers in each of the ten regions and the four supernodes. The supernode routers are located at Our Town (OT), Washington DC, City A, and City B. The regional routers are located in each of the USGA Region. A list of the Regions is contained in Table 1.

The supernode and regional routers are CISCO 7000 series routers that are connected together through T1 Backbone circuits. Each node is, at a minimum, connected to two other nodes. This forms the WAN backbone. The Internet connection is located at Their City, TS (See Figure 3-1).

The USGA Backbone has three external connections. The Internet connection is through a T3 circuit to an Internet service provider (ISP). The circuit connects to a fiber distribution data interface (FDDI) LAN with two NSC routers containing Transmission Control Protocol (TCP) filters. A T3 circuit from Their City to OT defines the path to the Internet. The supernode at OT has a NSC router that connects to a FDDI WAN. The WAN has both OT WAN and LAN routers that provide regional and local OT access to the Internet. The University of Our State (UOS) LAN connects to a CISCO router that limits access through filters to only one USGA server. The MCNC computer systems at 200 Park connect directly to the USGA network through a circuit to the OT FDDI LAN.

Table 3-1 Regional WAN Router Locations

Regions	Regional WAN Router Locations
Region 1	
Region 2	
Region 3	
Region 4	
Region 5	
Region 6	
Region 7	
Region 8	

The LAN routers that provide Tier III connection are a collection of CISCO 7000 series and 2500 series routers. The Tier I IBM mainframe connects to the network through the same NSC router used from connecting the T3 circuit from Their City.

The management of the network is monitored by an Integrated Network Management System (INMS) suite of computers. At the center of the INMS suite of computers is an HP XXX series computer with the HP OpenView application providing monitoring. The management of router configurations is through a collection of authorized (by IP address) computers located in OT Building XXX. This is where the network system administrators manage the network through Telnet sessions.

The ACC provides computer services to all USGA regional organizations. The Tier II computer services that are provided to USGA regional organizations through a collection of UNIX production systems. The UNIX production systems are listed in Table 3-2. They provide web services, e-mail services, and users services (applications and disk storage).

Table 3-2 UNIX Production Systems

UNIX System Name	UNIX Production System Platforms

In addition to the production systems, the ACC has UNIX non-production systems that are in various stages of configuration to eventually become production systems. Table 3-3 lists the non-production systems.

Table 3-3 UNIX Non-Production Systems

UNIX System Name	UNIX Non-Production System Platforms

The ACC E-Mail system is an integration of multiple E-mail packages. The main E-Mail package is DEC's All-In-One packages. This is running on dual DEC Vax XXXXs. Other e-mail packages include; CC-Mail, Groupwise, Lotus Notes, and Send Mail. The USGA Integrated Email system allows transfer among LAN Email systems. The backbone of the system is implemented on a central Digital Unix system running Digital Mailbus XXX software and send mail for message transfer/relay.

3.1.3 Tier III Architecture

Tier III consists of the workstations and remote terminals that are connected to the Tier I and II AIS resources described above. These workstations and terminals consist of a variety of personal computers and peripherals. Figure 3-4 shows the Tier III architecture. The Tier III systems consist mainly of Novell Netware 4.1 Servers. These servers are grouped as being Value Added Backbone Services (VABS) or User LANs. In addition, Tier III contains Windows-NT Servers that will be

brought online as production within the next month. All servers are configured based on a standard configuration, this provides consistence among the numerous servers.

The VABS are located throughout the USGA. Each USGA Region has a VABS providing support to the user LANs. All VABS are hosting Novell Netware 4.1. The VABS consists of: Locator; Postman; News; Application help; System Software Consolidation; and National/Local Applications.

User LANs provide access to the USGA architecture for all USGA employees. The User LANs include compact disk servers that act as data servers and additional application servers. The User LAN servers are in the process of being migrated from Novell Netware 3.x to 4.1. However, until this migration is complete, the Novell 4.1 servers will continue to support binary files.

There are two Windows-NT Servers going into the USGA architecture. They are both running version 3.5. One server is hosting a WWW page and the other is an Oracle server. The WWW page is closely coupled with the Oracle server.

3.2 Certification and Accreditation Boundary

The boundary for this C&A initiative is the boundary of the ACC facility in the ATC. The boundary is shown in Figure 3-2 Tier I Architecture. While some ST&E test Findings (Annex H-A, Appendix H) and SAV Observations (Annex H-B, Appendix H) may consider assets outside the immediate boundary of the ACC, those Findings and Observations will be included in the report due to their impact on ACC security.

SECTION 4. SYSTEM SECURITY REQUIREMENTS

4.1 Overview

The system security requirements (e.g., identification and authentication, contingency planning, access controls, etc.) are derived from National and USGA security policy. A Requirements Traceability Matrix (RTM) was constructed from the National and USGA level directives, and is included as Appendix D to this SSAA.

4.2 National Level Security Requirements

National level security requirements are derived from the documents listed in Appendix C Reference List.

4.3 Assignment of Responsibilities

A individual knowledgeable of the information technology used in the ACC AIS and in providing security for that technology has been assigned responsibility for security in each system. The Chief, ETSD has been designated as the Responsible Management Official. The Chief, Security Staff of ETSD is responsibility for the implementation of the program within ACC.

4.4 USGA Information Security Policy

USGA Information Security Policy is contained in Information Resources Management Manual. Chapter X, Information Systems Security, establishes a comprehensive, Agency wide security program to safeguard Agency AIS resources. The IRM Policy Manual sets forth the Agency's information security policy for both manual and automated systems and assigns individual and organizational responsibilities for implementing and administering the program.

The IRM Manual information security policy applies to all USGA organizations and their employees. It also applies to the facilities and personnel of agents (including contractors) of the USGA who are involved in designing, developing, operating, maintaining, or accessing Agency AIS resources. The system security policy for the ACC AIS resources is characterized by the following:

- Public Access to as much information as possible regarding Agency environmental initiatives.

- Restrict access to Agency AIS resources processing sensitive information to only those personnel with a valid authorization and need to know.

- Facilitate the open exchange of information to the fullest extent possible among authorized Agency users.

4.5 Security Plan

OMB A-130 requires the preparation of a Systems Security Plan and specifies the use of the OMB 90-08 format. USGA IRM XX provides additional Agency specific guidance. The information that would normally be included in an AIS Security Plan for the ACC is presented in a series Operational Directives contained in the ETSD Operational Directives Manual.

4.6 Review of Security Controls

Office of Management and Budget (OMB) A-130 Appendix III, requires the review of security controls in each system when significant modifications are made to the system. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system. OMB A-130 Appendix III also states the requirement to: "Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every three years."

USGA requires all new applications to undergo a control review leading to formal certification. Existing sensitive applications will be re-certified every three years. In instances where application safeguards are adequately defined within an installation's risk analysis, as described in the USGA Policy Manual Section X, separate application control reviews and certification/re-certifications are not necessary.

4.7 Authorization of Processing

The Director, ETSD, as the Responsible Management Official, is the knowledgeable management official who authorizes, in writing, the use of each general support system based upon implementation of its security plan before beginning or significantly changing processing in the system.

4.8 USGA Security Requirements

USGA security requirements are contained in USGA Directive, Information Security Manual. The specific requirements which pertain the AIS resources in the ACC are contained ETSD Operational Directives Manual. These requirements are presented in the form of Directives that address computer security program areas such as Management, Operational, and Telecommunications. Each area is further organized according to management functions, types of AIS, and telecommunications, respectively.

4.9 System Security Concept of Operations

The ACC security policy is enforced by the implementation, to the fullest extent possible, of Division C, Class C2 (C2): Controlled Access Protection as it is defined in the Department of Defense Trusted Computer System Evaluation Criteria, dated December 1985. This includes controlling access to systems processing sensitive information by using an identification and authentication (e.g., passwords), and using protection features such as discretionary access controls, individual accountability and auditing.

4.10 Network Connection Rules

The ETSD controls connections to the ACC AIS resources through the Operations Division.

SECTION 5. ORGANIZATIONS AND RESOURCES

This section pertains to the organizations and resources that are involved in the task of conducting the ACC C&A, and the contractual agreement that was entered into by those organizations. In June 1996, a representative from the USGA ACC Chief, Security Office met with representatives of the DISA Certification Division and determined that representatives from DISA's Certification and CAP Team would accomplish the USGA ACC audit.

The mechanism for the audit would be the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). The DITSCAP process provides the common framework to certify and accredit systems within the network infrastructures they employ. It also is used to maintain a documentation baseline of the security posture of these systems throughout their life cycle.

5.1 Identification of Organizations

The organizations responsible for performing, or supporting, the ACC AIS resource C&A process include USGA ETSD and the supporting contractor staff. The ETSD is responsible for ensuring compliance with the SSAA and the requirements stated therein. Other Agency staff may be called upon to support the C&A as defined below.

The development of the ACC SSAA and the activities associated with the ACC C&A are being accomplished by a C&A Team², which consists of representatives from the DISA, assisted by technical support contractors from CSC (Contract Number _____), TWM, and CORBETT Technologies, Inc.. The Delivery Order (DO) for these activities include the preparation of an ACC SSAA that can be used to accomplish the C&A of the ACC.

5.1.1 USGA ETSD Staff

The USGA Action Officer for this task order is Ms. Able. Ms. Able is the primary point of contact for the Team supporting this task. Her alternate is Ms. Jones. The USGA staff supporting this C&A process include those listed in Table 5-1.

Table 5-1 USGA ETSD Staff

Organization	Position and role	Function
USGA ETSD	Director ETSD (Acting)	Responsible Management Official
USGA ETSD	Chief, Security Staff	
USGA ETSD	USGA Action Officer	

5.1.2 The DISA C&A Team

The DISA C&A Team, was staffed and organized to complete all tasks in this delivery order (DO) on schedule, within budget, and in a timely manner. The team was supervised by Ms. Penny Klein, Task

² The word Team will be used to denote the USGA DISA and Contractor certification and accreditation project staff.

Manager (TM), who reports directly to the DISA INFOSEC Program Management Office (IPMO) Certification Section Manager, Mr. Jack Eller. Ms. Klein lead the technical task and was the principal liaison to the USGA Action Officer. Ms. Klein determined resource requirements and allocated team resources to the various tasks to meet the agreed upon schedule. Ms. Klein also recommended any required changes to task definition or schedule that were required.

Mr. Warner Brake, Test Director, lead the Security Test and Evaluation team composed of the DISA and contractor personnel.

DISA, CSC, CORBETT Technologies and TWM provided INFOSEC professionals to perform the C&A tasks as defined in the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). All team members pooled their efforts to accomplish the required task within the defined schedule.

Additional staff included the ABC Team's Quality Assurance Manager to insure a high quality product is delivered. Personnel supporting this delivery order were selected based on their technical qualifications, functional expertise, and knowledge of information systems environments.

5.2 DISA C&A Team Organizational Structure and Management Approach

The management and technical staff selected to support the USGA C&A Statement of Work (SOW) are depicted in the organization chart, Figure 5-1. The assigned Task Manager, Ms. Klein, will report directly to the USGA Action Officer for purposes of task coordination, direction, and progress reporting. Ms. Klein will establish and manage the cost accounts, budgets, schedules and deliverables.

Ms. Klein will meet monthly (or whenever necessary) with the USGA Action Officer, to review progress. Actual or potential problems will be identified and resolved following a structured process. Resource plans for task completion will be assessed to ensure the allocations are sufficient and optimal. The TM will receive weekly status reports from the Test Director and SSAA team. The TM will in turn provide weekly progress reports to the USGA Action Officer. Task impacts, including required resource and delivery schedule adjustments, will be coordinated with the USGA Action Officer.

5.3 Organizational Interfaces

The USGA Technical Task Manager for this C&A task is Ms. Able. Ms. Able is the primary point of contact for the C&A Team supporting this task. Ms. Able will review all deliverables to assure they adhere to the requirements established by the task and meet USGA standards. She will serve as the USGA technical representative for all tasks. The Task Manager, Ms. Klein, is responsible for ensuring that all contractual requirements of this task are met within the time and schedule agreed upon, and for coordinating activities with the USGA Action Officer.

Technical staff will be authorized direct contact with Government counterparts to obtain data or conduct tests as required by each task. Any commitments, schedule changes, or work method changes will be the responsibility of Ms. Klein.

<<<Insert Table 5.1 here>>>>

5.4 Resources and Roles

The primary assignments of team personnel are listed in Table 5-1. This table lists the contractor labor categories to be utilized and the personnel within those categories who are scheduled to perform the tasks as required under this delivery order. Key management, quality assurance, program and financial control, and support personnel were identified in Section 5.2 above.

All contractor personnel meet or exceed the requirements stated in the Personnel Qualifications of the prime contract. All staff resumes have been approved for work on this task. All of the contractor technical personnel assigned to this task have extensive experience in INFOSEC C&A and performance of tasks.

Ms. Klein, TM of this task, is responsible for the day-to-day operations of the task and the personnel assigned.

Assisting Ms. Klein are Mr. Warner Brake, Test Director; Ms. Keesha Perkins, test member; Ms. Maureen Premo, test member; Mr. Mark Wilson, NIST Observer; Senior INFOSEC Analysts Ms. Candice Stark, Mr. Barry Stauffer and Mr. Kenneth Rogowski. Mr. Brake is responsible for the ST&E testing planning, procedures, conduct and test report. Ms. Candice Stark is responsible for reviewing the SSAA, Security Test & Evaluation (ST&E) Test Plan, Procedures, Test Reports, and technical papers for their accuracy. Mr. Barry Stauffer and Mr. Kenneth Rogowski will provide expertise in the development of the USGA SSAA. Mr. Stauffer has been part of the DITSCAP development since its inception. Mr. Rogowski has extensive experience in the C&A of information systems and has recently successfully applied the DITSCAP process at the Drug Enforcement Administration.

To ensure the successful completion of this task, the TM has requested personnel experienced and knowledgeable in areas such as the DMC and DITSCAP objectives and a familiarity with large enterprise systems. Personnel will have knowledge of applicable security requirements and policies and shall have experience in the analysis of system security posture, performance of risk analyses, and preparation of policies, plans, and other documentation required to support the C&A of USGA systems and communications architecture. The DISA C&A Team has experience in the Federal Government and Defense Community with both unclassified but sensitive and classified systems, possess a full understanding of National information security requirements; are qualified in the use of automated hardware platforms, software, and databases; and are qualified in the use of physical and automated security measures to provide oversight and technical assistance. All assigned work will be coordinated with the task manager, Ms. Klein, and the USGA Action Officer to ensure agreement on approach and results.

5.5 Certification Team Experience

The USGA Certification and Accreditation team has extensive experience in the use of the DITSCAP. Ms. Klein, TM, has been extensively involved in the development and use of the DITSCAP. Mr. Brake, ST&E Test Director, has extensive C&A experience including the use of the DITSCAP on recent government initiatives. Mr. Stauffer and Mr. Wilkins were both members of the initial working

group that developed the DITSCAP. Both have successfully applied the DITSCAP. Mr. Stauffer and Mr. Rogowski are participating in the C&A of an office automation system, network control center, and classified information management system at the Agency ABC and have conducted a security evaluation for the Bureau of XYZ.

5.6 Other Supporting Organizations or Working Groups

Other USGA offices outside of the ETSD may be called upon to support the USGA ACC C&A. This support is specified in the Security Test Plan at Appendix G. The USGA Headquarters OIRM will provide required to provide interpretations of USGA computer security policies.

5.7 Administrative Issues

All text deliverables will be delivered in WordPerfect 6.1, graphics in MicroSoft PowerPoint 4.0, and spreadsheets in MicroSoft Excel 5.0. A diskette will be delivered with each technical deliverable.

SECTION 6. DITSCAP PLAN

6.1 Evaluation Approach

Overall Technical Approach. The Team's overall approach to the USGA C&A will use the DITSCAP.

The DITSCAP identifies four phases. These phases are: Definition; Verification; Validation; and Post Accreditation. These phases encompasses the life cycle of the system under review. In performing this task the USGA C&A Team will focus on the first three phases of the process.

Assumptions. This plan is based on the following assumptions:

- a. All data processed by the system is sensitive or below.
- b. A single USGA office is the Approving Authority and will approve the security requirements for the systems.
- c. The software employed in these systems is commercial software, not custom developed.
- d. The systems are operational, not under development, and thus not subject to design changes while the certification analysis is underway.
- e. The C&A effort is limited to the USGA ACC boundary as defined in Section 3.
- f. USGA representatives will be available to provide information during the data collection and evaluation stages and will participate in system security testing.

6.2 TASK 1: PROGRAM AND PROJECT MANAGEMENT

The TM will keep the Government Action Officer informed on progress through a variety of means. Informal technical discussions will be conducted between the USGA C&A team and the Government representatives on a near daily basis. This plan and the monthly status report are formal deliverables discussed below. The TM and others as deemed necessary will meet with the Government Action Officer to report on project activities, obtain guidance, or discuss problems periodically throughout the performance period. Meetings resulting in decisions or outlining action items will be documented in a report that will include agreements reached, action items opened, or issues closed.

The C&A team will provide general technical and administrative support and assistance in performing this DO. This includes, but is not limited to, attending meetings, reviewing documents, providing briefs and briefing materials, preparing trip reports, monthly activity reports, and other activities necessary to manage and coordinate the Certification and Accreditation effort.

6.2.1 C&A Task Order Management Plan

This C&A Management Plan is a living document that records the technical and management approach to be followed in satisfying the task objectives. The schedule, milestones and activities for each of the tasks and subtasks are portrayed in Appendix A of the Management Plan. Throughout execution of this

project the schedule will be updated to show progress against the plan. The schedule will be adjusted, as necessary, to reflect changes in direction provided by the Government or as a result of plan adjustments by the TM. The schedule will reflect both projected and actual plans and schedules.

6.2.2 Monthly Status Report

The monthly status report will be delivered on the 17th day of each month. The technical portion of the report will include accomplishments, plans, travel, meetings conducted, and areas of concern for each task area. The planning information will be derived from the plans and schedule documented in this plan. The report will include funds planned vs. expended to date, funds remaining, and any areas of concern.

6.2.3 Trip Reports

The team will provide a Trip Report to the Government whenever travel is performed in relation to a project. The trip report shall contain the purpose of the trip, the trip dates, location of the trip, who was visited during the trip, major accomplishments of the trip, tasks or follow-up activities that are required as a result of the trip.

6.3 TASK 2: USGA C&A Support

The DITSCAP encompasses four phases: Definition, Verification, Validation, and Post Accreditation. Phase I, **Definition**, focuses on understanding the mission, environment, and architecture to determine the security requirements and level of effort necessary to achieve accreditation. Phase II, **Verification**, verifies the evolving, or modified, system's compliance with the agreed upon security requirements. Phase III, **Validation**, validates the fully integrated system's compliance with the security requirements. Phase III concludes with full approval to operate the system, e.g., security accreditation. Phases I, II, and III are the DITSCAP process engine. These phases are repeated as often as necessary to produce an accredited system. Phase IV, **Post Accreditation**, includes those activities necessary for the continuing operation of the accredited system. The objective of Phase IV is to ensure system management, operation, and maintenance to preserve an acceptable level of residual risk. In accomplishing this Delivery Order, the team will perform the first three phases of the DITSCAP.

6.3.1 SUBTASK 2.1: Definition Phase

During the Definition Phase, the C&A Team will attend technical meetings and collect data on the system architecture. The C&A team will develop a draft SSAA which defines the system operating and threat environment; describes the system and the certification boundaries; defines the security requirements, Security Policy, and security Concept of Operations; and provides a Certification Plan. A RTM will be developed to document all security requirements applicable to the USGA system under consideration. This draft will then be available for review by the USGA Program Manager and the DAA.

The Team will perform a quick and high level review of the system to understand the macro issues. The Team will place boundaries around the work, emphasizing the vulnerabilities at the interfaces, and partition the certification work within those boundaries. The Team will then identify areas of emphasis which begin to emerge from the boundary definition and partitioning, areas of concern which must

receive management focus during the certification and begin drawing up the DITSCAP plan. The DITSCAP SSAA document preparation will begin.

The Team will assist in the USGA Site Security Assessment Visits (SAV). The SAV will be used to collect data to determine the scope of certification effort required, the level of personnel expertise, the experience necessary to perform certification activities, and determine the need for testing of the network operations center at vendor locations. During the SAV visits, the Team will gather sufficient documentation to enable development of the required Certification Plan. Prior to the SAV, the Team will develop recommendations for determining effective and efficient methods of assessing information technology security posture. These findings will be presented to DISA in a Technical Report.

Next the Team will develop a RTM showing the documented security requirements as defined in Section 4 of this SSAA. The RTM includes: directives, requirements, technical controls, infrastructure safeguards, method of certification (e.g., testing, inspection), and compliance, and assurance entries. The RTM identifies all the security requirements for the system. As the work progresses, each requirement will be traced to specific safeguards (practices, procedures, hardware, software, or firmware) which will satisfactorily fulfill the requirements. Any requirement not satisfactorily fulfilled results in a vulnerability.

6.3.2 SUBTASK 2.2: Verification Phase

During the Verification Phase, the C&A Team will continue to collect data on the system architecture and analyze the ability of the system to provide the requisite security. The Team will review the documented security requirements to determine whether system safeguards, both infrastructure and application, address the security requirements. The activities of this phase verify the system's compliance with the requirements agreed on in the RTM. Activities include continuing refinement of the SSAA, system development or modification, and certification analysis. Phase II starts with a review and, if necessary, refinement of the SSAA. As the development or modification progresses and specific information relating to the certification effort becomes available, the SSAA is updated to include more specific details. As details about the hardware and software architecture become available, this information is added to the SSAA to support the agreed upon level of certification actions.

The certification activities verify by analysis, investigation, and comparison that the system design implements the security requirements and the security critical components function properly. Six certification actions or tasks are performed during this phase. These include:

- System Architecture analysis that verifies that the system architecture complies with the architecture description agreed upon in the SSAA.
- Software Design analysis that evaluates how well the software implements the security requirements of the SSAA and the security architecture of the system.
- Network Connection Rule Compliance analysis that evaluates connections to other systems and networks to ensure the system design will enforce security policies.
- Product integrity analysis that evaluates the integration of non-developmental software, hardware, and firmware to ensure their integration complies with the system security architecture, and the integrity of each product is maintained.

- Life Cycle Management analysis that verifies that change control and configuration management practices are, or will be, in place and are sufficient.
- Vulnerability Assessment that evaluates security vulnerabilities and recommends appropriate countermeasures.

In some cases the technical meetings will be conducted onsite as part of a Security Assessment Visit (SAV). The C&A team will continue to refine the system and network architecture. The ST&E Plan and Procedures will be developed. The ST&E Plan at Appendix G defines a procedure (document review, interview, system test, or observation) to test compliance with each requirement in the RTM. A Risk Analysis will be conducted and the results will be included in an appendix to the SSAA.

Once the SAV is complete the C&A Team will support all facets of the ST&E. These activities include reviewing existing vendor security test to determine which procedures can be used to augment the ST&E Plan and Procedures. In addition, the C&A Team will Develop ST&E Plan and Procedures. During the ST&E the C&A Team will support the government test director in the execution of the ST&E. As findings are identified they will be provided to the test director into a Technical Report at Appendix H. The test findings and test result notes will enable the test director to prepare the ST&E Report.

At the completion of the Certification Analysis, the system will have a documented security specification, a comprehensive test plan, and assurance that all network and other interconnections requirements have been implemented. A vulnerability assessment will have been conducted and will have concluded that the infrastructure needs of the system, e.g., configuration management, will be accommodated throughout the system life cycle. An initial Statement of Residual Risk will be prepared.

6.3.3 SUBTASK 2.3: Validation

During the Validation Phase, the C&A Team will evaluate the system operations and support DISA in the conduct of the ST&E and preparation of the test report. This includes all pre and post technical meetings required. A System Security Evaluation Report at Appendix I will be prepared to combine the results of the SAV observations and issues (see Annex H-B and Annex H-C of Appendix H) and the ST&E, define areas of residual risk and provide recommendations of actions necessary to effectively counter the residual risk. This report will be included in the final SSAA.

Activities of this step validate that preceding work has produced a system that operates in a specified computing environment with an acceptable level of residual risk. Certification Evaluation of the integrated system includes eight actions to certify that the fully integrated system is ready for operational deployment. These actions include:

- System Security Testing and Evaluation to assess the technical and nontechnical implementation of the security features and their proper performance.
- Penetration Testing, for appropriate system classes, may be useful to assess the system's ability to withstand attempts to circumvent system security features.

- TEMPEST and Red/Black Verification may be required to validate that the equipment and site meet the security requirements.
- Validation of COMSEC Compliance to validate that COMSEC approval has been granted and approved COMSEC key management procedures are used.
- System Management Analysis that examines the management infrastructure to determine if it will maintain the mission, environment, and architecture described in the SSAA.
- Site Accreditation Surveys to validate that the operational procedures for the information technology, environmental concerns, and physical security pose no unacceptable risks.
- Contingency Plan examination that analyzes the contingency and continuity of service plans to ensure they are consistent with the SSAA.
- Risk Management Review that assesses the operation of the system to determine if the risk is being maintained at an acceptable level.

This task will conclude with the preparation of the System Security Evaluation Report following the format of the DITSCAP SSAA and the specified DID.

Report Of Findings. At this point the Team documents the results of the C&A effort with a completed SSAA. It will summarize the applied security standards and policies, and detail the vulnerabilities, controls, corrective actions, operational restrictions and certification process used. The SSAA will contain both the technical and management security recommendations for the systems. The final Statement of Residual Risk and System Security Evaluation Report will be included in the completed SSAA following the DITSCAP format and the specified DID's.

The final step for the team is to document the results of the certification effort with an Accreditation Statement that is contained in an Appendix. This statement will explicitly record the acceptance of the residual risk. A specific mitigation strategy will be reviewed with the USGA staff and recommended to the USGA DAA.

6.4 Schedule summary

The schedule of security activities has been developed in MicroSoft Project. This project plan of the certification analysis and other events that lead to an accreditation schedule is presented in Appendix E - Certification and Accreditation Project Work Plan of this SSAA.

Schedules for the project are found in Table 6-1 which shows deliverables with DID number and scheduled delivery dates.

Table 6-1 Deliverable Schedule

Deliverable Title	CDRL/DID #	Calendar Days after DO Start	Date Due
Delivery Order Management Plan	A003/ DI-MGMT-80347	15	Draft _____ Final _____
Monthly Status Report	A002/ DI-MGMT-80368	30	15th of each month
Report/Minutes, Record	A010/ UDI-A-23083A		5 days after event
Technical Report	A005/ DI-MISC-80508	As required	As Required
System Security Authorization Agreement (SSAA)	A005/ DI-MISC-80508	21 days from COR/TIM notification	Version 1.0 _____ Version 2.0 _____ Version 3.0 _____
Security Test and Evaluation (ST&E) Test Plan and Procedures	A0026 DI-NDTI-80566	60 days from COR/TIM notification	With Version 2.0 of SSAA
Certification Plan	A005/ DI-MISC-80508	30 days from COR/TIM notification	With Version 1.0 of SSAA
Security Policy	A005/ DI-MISC-80508	30 days from COR/TIM notification	With Version 1.0 of SSAA
Security Concept of Operations	A005/ DI-MISC-80508	25 days after TIM notification	With Version 1.0 of SSAA
Trip Report	A010	10 days after completion of TDY	

A contractor detailed schedule and work plan has been developed in Microsoft Project. This plan is presented in Appendix A - Contractor Project Work Plan of the Deliver Order Management Plan.

Appendix A: Acronym List

ACC	Agency Computer Center
AIS	Automated Information System
ATC	Agency Technology Center
C&A	Certification & Accreditation
CAI	Confidential Agency Information
CBI	Confidential Business Information
CMP	Configuration Management Program
CONUS	Continental United States
CSSO	Computer Systems Security Officer
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DEC	Digital Equipment Corporation
DID	Data Item Description
DISA	Defense Information System Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
E-Mail	Electronic Mail
ETSD	Enterprise Technology Services Division
FDDI	Fiber-Optic Data Distribution Interface
FIPS	Federal Information Processing Standard
GFE	Government Furnished Equipment
GFI	Government Furnished Information
HP	Hewlett Packard
I & A	Identification and Authentication
INFOSEC	INformation System SECurity
INMS	Integrated Network Management System
IPMO	INFOSEC Program Management Office
IRM	Information Resource Management
ISSO	Information Systems Security Officer
LAN	Local Area Network
LPAR	Logical Partitions
NACI	National Agency Check with Inquiries
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI 4009	National Security Telecommunications and Information Systems Security Instruction Glossary
OMB	Office of Management and Budget
OT	Our Town
PM	Program Manager
POC	Point of Contact
RACF	Resources Access Control Facility

RMO	Responsible Management Official
RTM	Requirements Traceability Matrix
SAV	Security Assessment Visit
SBU	Sensitive But Unclassified
SOW	Statement Of Work
SSAA	System Security Authorization Agreement
ST&E	Security Test and Evaluation
TCSEC	Trusted Computer Security Evaluation Criteria
TCP/IP	Transmission Control Protocol/Internet Protocol
TELNET	Text-based protocol for logging on to remote servers
TIM	Technical Interchange Meeting
TM	Task Manager
UOS	University of Our State
USGA	U. S. Government Agency
USERID	User Identification
WAN	Wide Area Network
WWW	World-Wide Web

Appendix B: Glossary of Terms

The terms used in the USGA ACC SSAA were selected from USGA policy and directives, or National Security Telecommunications and Information Systems Security Instructions (NSTISSI) 4009 definitions. A complete list can be found at Appendix XX, USGA IFM.

Appendix C: Reference List

Information Security References

The references listed below is an extract of the major reference information contained in Appendix D of USGA ISM XXXX.

1. CFR Part 17 - National Security Information Program
2. Computer Security Act of 1987 (P.L. 100-235), 8 January 1988
3. Office of Management and Budget Circular No. A-123, Management Accountability and Control, June 21, 1995
4. Office of Management and Budget Circular A-130, Appendix III - Security of Federal Automated Information Resources, February 1996
5. Office of Management and Budget Bulletin 90-08, Individual Security Plan Guidance
6. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4001 - Controlled Cryptographic Items (FOUO)
7. Federal Information Processing Standard 112, "Password Usage"
8. Federal Information Processing Standards (FIPS) Publication, 102, Subject: Guideline for Computer Security Certification and Accreditation, September 27, 1983.
9. Chapter X, USGA IRM Policy Manual, dated _____.
10. USGA Information Security Manual.
11. Office of Administration and Resources Management, Agency Data Processing Division, Our Town.
12. Office of Administration and Resources Management, Agency Data Processing Division, Our Town, USGA Internet Security Review.
13. Network Policy, Threats, and Controls, prepared by W. Timothy Polk, National Institute of Technology, dated April 21, 1994.
14. NIST SPEC PUB 800-10, Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls, December 1994.
15. DoD 5200.28-STD, Department of Defense Standard, Subject: Department of Defense

Trusted Computer System Evaluation Criteria, dated December 1985

16. ETSD Operational Directives Manual.

Appendix D: Requirement Traceability Matrix

The enclosed matrix contains the parsed requirements related to the USGA - ACC AIS resources.

Appendix E: USGA - ACC Certification and Accreditation Work Plan

The chart contained at this Appendix shows an overview of the work performed during the development of the USGA ACC SSAA, Version 3.0. The chart was prepared using the MicroSoft Project software application, and is an extract from the work plan that contains the schedule of security activities for the certification and accreditation of ACC AIS resources is part of the Task Order Management Plan.

Appendix F: Risk Assessment

This Appendix include information that pertains to the risk assessment of the ACC AIS resources. The risk assessment of the IBM mainframe environment was performed was performed during 199_. The results of those assessments are on file in the ETSD.

Appendix G: Security Test and Evaluation Test Plan and Procedures

This section contains the Security Test and Evaluation Test Plan and Procedures for the USGA-ACC Minimum Security Requirements.

Appendix H: Security Test and Evaluation Test Evaluation Report

This section contains the Security Test and Evaluation Test Evaluation Report for the USGA ACC Minimum Security Requirements. The results of the tests conducted using the Security Test Plan and test procedures are reported in the Security Test Report at Annex H-A in terms of Findings. The results of the Security Assistance Visit # 1 are presented in Annex H-B in terms of Observations, and the results of Security Assistance Visit # 2 are contained in Annex H-C in terms of Issues. The relationship between the RTM and the Findings, Observations and Issues is shown in the RTM at Appendix D.

Appendix I: System Security Evaluation Report

This section contains the System Security Evaluation Report for the USGA ACC Minimum Security Requirements. It contains the consolidated analysis of information presented in the Security Test and Evaluation Report (See Appendix H).

Appendix J: Certification Statement

This Appendix contains an USGA ACC Certification statement.

Certification Statement

We have extensively examined the USGA ACC AIS and network resources and the Findings, Observations and Issues documented in the final ACC System Security Authorization Agreement (SSAA), Version 3.0, dated April 30, 1997 with the enclosed System Security Evaluation Report at Appendix I.

The ACC AIS and network resources were evaluated for compliance with the Federal Statutes, regulations, and applicable Agency policy and directives as identified in Appendix D of the ACC SSAA. With the exceptions noted in Appendix I of the ACC SSAA, we certify that the USGA ACC AIS and network resources meet or exceed the requirements. Residual Risks remaining are described in Appendix I.

In view of the Residual Risks, we recommend the USGA ACC system be granted an interim certification for three months to provide an opportunity for satisfactory resolution of the Findings, Observations and Issues delineated in Appendix H of the ACC SSAA, Version 3.0. When these Findings, Observations and Issues have been satisfactorily resolved, the USGA ACC system will be granted a full certification.

_____ Date _____ Date

Appendix K: ACC Security Operating Procedures Guide

The security operating procedures which pertain the AIS resources in the ACC are contained ETSD Operational Directives Manual. These procedures are presented in the form of Directives that address computer security program areas such as Management, Operational, and Telecommunications. Each area is further organized according to management functions, types of AIS, and telecommunications, respectively. These directives are on file in ETSD, where they are available for review.

Appendix L: Approval to Operate

This section contains the Approval to Operate statement prepared by the Resource Management Officer.

Approval to Operate Statement

Date

I have carefully examined the USGA ACC system Certification Findings, Observations and Issues documented in the final ACC System Security Authorization Agreement (SSAA), Version 3.0, dated April 30, 1997.

Based on my authority and judgement, and weighing the residual risks against operational requirements, I authorize the interim operation of the ACC AIS and network resources for three months to provide an opportunity for satisfactory resolution of the issues delineated in Appendix H of the ACC SSAA, Version 3.0. When these issues have been satisfactorily resolved, the ACC will be granted a full accreditation.

Division

Mr. Jones
Director, Enterprise Technology Services

US Government Agency

Appendix M: Rules of Behavior

The information in this section pertains to the Rules of Behavior that have been prepared by ETSD for ACC users. Additional information regarding these rules can be obtained from Chief, ETSD.

Appendix N: Security Awareness and Training Program

This section will contain information that pertains to the ETSD security awareness and training program. Additional information can be obtained from Chief, ETSD.

Appendix O: Incident Response Program

Information pertaining to the ETSD incident response program can be obtained from Chief, ETSD.

Appendix P: Continuity of Support

Information pertaining to the Disaster Recovery and Disaster Recovery for the ACC can be obtained from Chief, ETSD.

Appendix Q: Interagency Agreements

This section contains information pertaining to Interagency agreements between USGA and other federal, state and local government agency's and offices that pertain to AIS support provided to those offices by the ACC. Additional information on these agreements can be obtained from the Chief, ETSD.